Possehl Secure

SECURITY FACTORY / DETECT & RESPOND

SECURITY OPERATIONS CENTER (SOC) – CYBER-KRIMINELLEN EINEN SCHRITT VORAUS

Die Kombination aus präventiven Schutzmaßnahmen, frühzeitiger Erkennung von Angriffen und einer effektiven Kontrolle ist heute essenzieller denn je. Die geeignete Technologie und damit verbunden die zugehörigen Skills und Prozesse in Eigenregie aufzustellen, ist für viele Unternehmen sehr anspruchsvoll. Um Unternehmensressourcen zu schützen, bedarf es einer modernen, kontinuierlich geprüften und integrativen Sicherheitsarchitektur.

Ein professionelles Security Operations Center (SOC) bietet Ihnen ein kontinuierliches, effizientes Sicherheitsmonitoring sowie einstudierte und erprobte Reaktionen auf potenzielle Cyberangriffe. Zudem werden wichtige Anforderungen aus Best-Practice-Frameworks (bspw. CIS Control insbesondere Control 8, 10 und 13) und Regulatorik (bspw. NIS2 und DORA) adressiert.

Unsere Lösung

Das Possehl Security Operations Center überwacht mit modernster Technologie und hoch spezialisierten, vertrauenswürdigen Experten Ihre digitale Angriffsfläche.

- In Deutschland ansässiges Security Operations Center
- Experten im Bereich der offensiven und defensiven Sicherheit
- Langjährige Erfahrung in mittelständischen und Enterprise Umgebungen

Wir analysieren Ihre bestehende IT-Sicherheitsarchitektur und entwickeln ein passgenaues SOC-Konzept. Dabei bleiben Sie flexibel: Sie können Ihr eigenes SOC optimieren oder bestimmte Aufgaben an Possehl Secure auslagern. Im Falle eines Managed Security Operations Centers definieren wir Anforderungen, Service Levels und KPIs höchst individuell.

Security Operations Center Tech Stack

Je nach Anforderung und Komplexität der Infrastruktur sowie Risikolage kommen innerhalb des Security Operations Centers verschiedene Technologien zum Einsatz.

Schwachstellenmanagement

Kontinuierliche Prüfung der eingesetzten Software und Firmware auf mögliche Schwachstellen sowie risikobasierte Priorisierung für gezielte Behebung im Patchmanagement.

Endpoint Detection & Response (EDR/XDR)

Automatisierte Überwachung und Angriffserkennung direkt an den Endpunkten.

Security Information und Event Management (SIEM)

Als zentrale Plattform unseres SOC korreliert das SIEM sicherheitsrelevante Daten, integriert EDR und Schwachstellenmanagement und ermöglicht eine strukturierte Analyse und Incident Response.

Risiken und Fehler lassen sich nie ganz vermeiden. Doch durch eine abgestimmte, mehrschichtige Sicherheitsarchitektur und ein kontinuierliches Monitoring können Bedrohungen frühzeitig erkannt und eingedämmt werden.

Phasen der Implementierung

Da die IT-Umgebungen, die schützenswerten Güter, die regulatorischen Anforderungen und schlussendlich auch die Budgets unserer Kunden unterschiedlich sind, entwerfen wir eine höchst individuelle und anforderungsgerechte Architektur inkl. dazugehöriger Technologie und Service-Level.

1 SECURITY OPERATIONS CENTER WORKSHOP
Bedrohungs-, Reifegrad- und GAP-Analyse, Analyse der Architektur und Schwachstellen, SOC Blueprint (Produktauswahl, Konzipierung und Architektur)

2 ROLLOUT DER SECURITY OPERATIONS CENTER LÖSUNG
Rollout on Premises oder in der Cloud und Anbindung spezifischer Datenquellen

3 PRÜFUNG DER EFFEKTIVITÄT
In zeitlichen Abständen werden immer wieder gezielt simulierte Angriffe mit rotierenden Vektoren und Werkzeugen auf die Umgebung durchgeführt.

4 BETRIEB DES SECURITY OPERATIONS CENTERS
Eigenbetrieb, hybrider Ansatz oder SOC as a Service

SOC-AS-A-SERVICE / MANAGED SERVICE
Kontinuierliche Überwachung der Umgebung und Reaktion auf Security Incidents durch Possehl Secure Experten. Nach der Inbetriebnahme werden Sie kontinuierlich mit relevanten Informationen zu Angriffen und der Qualität des Services versorgt. Optional erhalten Sie Zugriff auf ein Security-Cockpit, in dem der Zustand der Umgebung eingesehen werden kann.

5 KONTINUIERLICHER VERBESSERUNGSPROZESS
Effektivitätstests, Cyber Incident Simulationen

Ihr Nutzen – Unser Mehrwert

Unsere Philosophie beruht auf einer 360°-Sicht auf IT-Sicherheit, herstellerneutraler Beratung und einer partnerschaftlichen Zusammenarbeit auf Augenhöhe. Unser Ziel ist es, Ihnen eine maßgeschneiderte, zukunftssichere Sicherheitslösung zu bieten, die Ihr Unternehmen nachhaltig schützt.

Mehr zum Security Operations Center Workshop finden Sie unter:

www.possehl-secure.de/security-operations-center

Die **Possehl Secure GmbH** ist Ihr Partner im Bereich der Cybersecurity. Mittleren und großen Unternehmen aller Branchen bieten wir maßgeschneiderten Service und kundenorientierte Lösungen. Damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

vertrieb@possehl-secure.de | T +49 221 466 195-20 | www.possehl-secure.de

05/2026